

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Jamie West, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I am a Special Agent with Homeland Security Investigations (HSI). HSI is a directorate within Immigration and Customs Enforcement (ICE). ICE is a subordinate component of the Department of Homeland Security (DHS) and the successor to many of the law enforcement powers of the former Immigration and Naturalization Service and the former U.S. Customs Service. I have been a Special Agent since January 2002 and I am currently assigned to HSI Derby Line, Vermont. I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center and work relating to these types of investigations. I have had discussions with other law enforcement officers about how people use computers to commit crimes and the law enforcement techniques that can be utilized to investigate and disrupt such activity. I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. As a Special Agent, I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7). I am empowered to conduct

investigations of and to make arrests for offenses involving the sexual exploitation of children enumerated in 18 U.S. § 2251 *et seq.*, and for other felony offenses.

3. As a Special Agent, I know that 18 U.S.C. § 2252(a)(4)(B) prohibits a person from possessing images of children engaged in sexually explicit conduct, as defined in 18 U.S.C. section 2256 (“child pornography”), and 18 U.S.C. § 2252(a)(2) prohibits the receipt and distribution of child pornography.

4. I make this affidavit in support of an application for a warrant to search the following:

(1) A Lenovo IdeaPad U510 laptop computer, model: 20191, serial number CB20422712 (the “Subject Device”).

(2) Any extraction(s) to include logical and/or physical images (hereinafter referred to as the “Subject Image(s)”) conducted by U.S. Probation of the Subject Device. All these items are currently stored at the U.S. Probation office in Burlington, Vermont.

5. I have not included every fact known to me concerning this investigation. I have set forth only those facts which I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B) will be found on the Subject Device and/or Subject Image(s). As outlined below, and based on my training and experience, I believe that there is probable cause to believe that evidence, fruits, and/or instrumentalities of the aforementioned crimes are located on the Subject Device and/or Subject Image(s).

6. The statements contained in this affidavit are based upon my investigation, information provided to by other law enforcement officers and witnesses, and on my training and experience as a Special Agent.

LEGAL BACKGROUND

DEFINITIONS

7. The following definitions apply to this Affidavit and attachments hereto:

a. “Child Pornography,” as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

c. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to,

keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

f. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software

or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. “Internet Relay Chat” (“IRC”) is a method of engaging in group communication and private communication over the Internet. A user installs a computer program (“client”) that allows him or her to communicate through a network of computers. Most IRC communication occurs in discussion forums, called channels. One-on-one communication via private messages, chat, and direct data transfers are also possible using most clients. Direct data transfers can include the sharing of digital files, including videos and photographs.

i. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including telephone based dial-up, broadband based access via digital subscriber line (“DSL”) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which

the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system, or via satellite, and can access the Internet by using his or her account name and personal password.

j. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

k. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

l. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such

as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMCs”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

m. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

n. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

o. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (“HTML”) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (“HTTP”);

#### PROBABLE CAUSE

8. I have spoken with U.S. Probation Officer (USPO) Jon Hansen regarding Gregory Gochie. From these conversations and from my own personal knowledge, I know the following:

a. USPO Hansen is responsible for supervising Gregory Gochie. In 2015, Gochie was convicted of Failure to Register under the Sex Offender Registration

and Notification Act (SORNA) in federal court in Vermont and was sentenced to serve a sentence of 63 months followed by 10 years of supervised release, with an additional 24 month consecutive term of imprisonment for a violation of supervised release. One condition of Gochie's current term of supervised release bars him from possessing adult and child pornography. Another condition permits probation officers to search Gochie's property, including computers and electronic devices without a warrant, based upon "reasonable suspicion concerning a violation of a condition of supervised release."

b. On or about June 8, 2021, Gochie was arrested by the U.S. Marshal's Service in Brownington, Vermont and charged with failure to report to his Probation Officer, failure to report change of address, and failure to attend sex offender treatment.

c. Also on June 8, 2021, Jon Hansen traveled to Brownington, Vermont and met with Marion Dubois. Dubois advised Hansen that Gochie lived with her at her residence. She provided Hansen with the Subject Device and advised him that it belonged to Gochie and that he had used it to view pornography. Hansen took possession of the Subject Device. The Subject Device was later reviewed by U.S. Probation Office Forensic Examiner Jeremy Wandasiewicz.

d. On or about August 6, 2021, U.S. Probation alerted Homeland Security Investigations to the discovery of possible child exploitation material on the Subject Device.

9. In August 2021, I met with Wandasiewicz. Wandasiewicz advised that, during a search of the Subject Device, he had located several files that may contain child exploitation



material. I have reviewed the files Wandasiewicz discovered. Two of the images are described as follows:

a. File 000000004797.JPG is an image file depicting a nude female lying on her back. She has some breast development. The photograph shows the female only from the waist up.

b. File 000000006895.JPG is an image file depicting two females who appear to be adolescents sitting on a couch. The female on the left side of the photograph is wearing a bra and underwear. The female on the right side of the photograph is wearing a bra and no underwear. She is sitting, with her legs spread on a male's lap and it appears the two are engaged in intercourse. The male's right hand is covering most of the female's genital area and he appears to be touching the female's genitals.

10. Wandasiewicz saved the Subject Images to a portable device and provided it to me. I sent the Subject Images to the National Center for Missing and Exploited Children (NCMEC) to compare them with previously identified victims. NCMEC later advised that none of the images appeared to contain any identified series.

11. Wandasiewicz also advised me that, during a search of the internet browsing history on the Subject Device, he found the following search terms: "doll faced teen porn", "tight young pussy porn", "teen porn", "young pussy porn", "retarded girl porn", "young tender pussy porn", "hairy teen pussy", and "fucking retarded girls."

12. On September 2, 2021, I met with Joseph Hagen, Jr, a clinical professor in pediatrics at the Lerner College of medicine at the University of Vermont and a primary care pediatrician at Lakeside Pediatrics in Burlington, Vermont. I showed Dr. Hagen the Subject

Images and asked him to estimate the age of the females. Dr. Hagen provided a report in which he described each image and provided an age for females in two of the three images.

a. Dr. Hagen opined that, based on the facial structure, muscle development, and breast development using the Sexual Maturity Rating (SMR), the female in image 000000004797 is less than 16 years old.

b. Dr. Hagen advised that, using the SMR, he believes the female who is not wearing underwear in the image 000000006895 “is certainly under 16 years of age and she is the victim of rape” – even though the image does not appear to depict the male using force to overcome resistance from the minor.

13. Based on my conversation with Dr. Hagen, I believe that the girl in file 000000006895 is under the age of 18, and thus is a minor as defined by federal law. I also believe that the image depicts child pornography.

#### BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

14. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and my experience as a Special Agent, I know the following about computers and computer technology:

a. Computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed. Basically, computers serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

b. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

c. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

d. The Internet affords individuals several different venues for meeting each other, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

e. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be

intentional, for example, by saving an email as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer to peer (P2P) file sharing software, when the computer was sharing files, and some of the files that were uploaded or downloaded.

- i. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or "slack space," that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a

record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits. Wholly apart from user-generated files, computer storage media – in particular, computers’ internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it (user attribution). To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

f. File transfers and online connections occur to and from IP addresses.

These addresses are unique to particular computers during online sessions. An IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred between computers.

g. Third-party software is available to identify the IP address of a particular computer during an online session. Such software monitors and logs Internet and

local network traffic. It is possible to identify the person associated with a particular IP address through ISP records. ISPs maintain records of the IP addresses used by the individuals or businesses that obtain Internet connection service through the ISP. Those records often include identifying and billing information, account access information in the form of log files, email transaction information, posting information, account application information, and other information both in computer data and written record format.

#### CHARACTERISTICS OF CHILD PORNOGRAPHERS

15. Based upon my knowledge, experience, and training in child exploitation investigations, I know that there are certain characteristics common to individuals involved in such crimes:

- a. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and

gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

- c. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child-pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.
- e. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material related to children; and often maintain lists

of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

- f. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. As a result, I submit that there is probable cause to believe that records, documents, and materials stored on the Subject Device and Subject Image(s) that constitute evidence of violations of 18 U.S.C. §§ 2252(a)(2) and (a)(4)(B).

16. As further described in Attachment B, this application seeks permission to locate not only computer files, records, documents, and materials that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the Subject Device was used, the purpose of its use, who used it, and when.

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record



additional information, such as the attachment of peripherals, the attachment of USB flash storage Device or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created, and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus spyware and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts,

electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

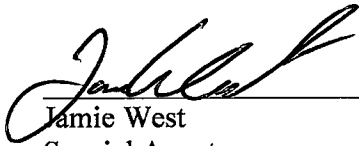
- c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- d. Further, in finding evidence of how an electronic device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

17. Because this warrant seeks only permission to examine the Subject Device and Subject Image(s), which are already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

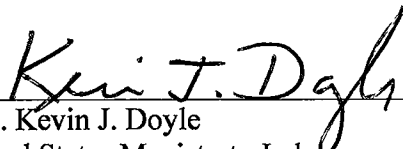
18. Based on the foregoing, I submit probable cause exists to search the Subject Device and Subject Image(s), more specifically described in Attachment A, for the evidence delineated in Attachment B.

Dated at Burlington, in the District of Vermont, this 4th day of October, 2021.



Jamie West  
Special Agent  
Homeland Security Investigations

Sworn to and subscribed before me on this 4th day of October, 2021.



Hon. Kevin J. Doyle  
United States Magistrate Judge